GarrettCom
Ethernet at Its Best™

Magnum 6K25 Switches

Software User Guide

MNS-6K

GarrettCom, Inc.
213 Hammond Ave.
Fremont, CA 94539
Phone: (510) 438-9071
Fax: (510) 438-9072

Email: support@garrettcom.com

www.GarrettCom.com

Preface

Use of This Guide

This guide describes how to use the command line interface (CLI), for the Magnum 6K25 Switches.

If you need information on a specific command in the CLI, type the command name after you type the word “help” (help <*comman*d>) or just type <command> [Enter].

If you need further information on GarrettCom switch technology, refer to the GarrettCom website at:

http://www.garrettcom.com

Magnum? 6K-Series

6K25 Switch Software
(MNS)

Software User Guide

Part #: 84-00130

Trademarks

Ethernet is a trademark of Xerox Corporation

NEBS is a trademark of Telcordia Technologies

UL is a registered trademark of Underwriters Laboratories

GarrettCom, Magnum and **Personal Switch** are trademarks and **Personal Hub** is a registered trademark of GarrettCom, Inc.

Copyright ? 2001 GarrettCom, Inc. All rights reserved. No part of this publication may be reproduced without prior written permission from GarrettCom, Inc.

Printed in the United States of America.

Contacting GarrettCom, Inc

Please use the mailing address, phone and fax numbers and email address listed below:

GarrettCom, Inc.

213 Hammond Ave.

Fremont, CA 94539

Phone (510) 438-9071

Fax (510) 438-9072

Website: http://www.GarrettCom.com

Email: support@garrettcom.com

Federal Communications Commission

Radio Frequency Interference Statement

This equipment generates, uses and can radiate frequency energy and if not installed and used properly, that is in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

Table of Contents ..... Page

1.1 Getting Started with Switch Configuration 7
1.2 Software Upgrade 7
1.3 Recommended Minimal Configuration 7
1.4 Using the Console Setup Screen 7
1.5 To Recover from a Lost Manager Password: 8
2.0 CONSOLE MANAGEMENT INTERFACE 9
2.1 Understanding Management Interfaces 9
2.2 Console Port Connection 9
2.3 Advantages of Using the CLI 10
2.4 CLI Usage 10
3.1 Accessing the CLI 11
3.2 Using the CLI 11
3.3 Privilege Levels at Logon 11
3.4 Listing Commands and Command Options 12
3.4.1 Operator Privilege 12
3.4.2 Manager Privilege 12
3.4.5 Displaying Help for an Individual Command. 13
3.4.7 Displaying Help with all possibilities. 14
4.1 IP Configuration 15
4.1.1 IP Address and Subnet Mask. 15
4.1.2 Default Gateway Operation 15
4.2 A Quick Start 15
4.3 Interface Access: Console/Serial Link, Features 15
4.4 System Information 15
4.4.1 System Contact and Location: 16
4.4.2 Time Zone: 16
4.5 CLI: Listing the Current System Information. 16
4.5.1 List the current system information settings. 16
4.5.2 Configure the Time Zone and Daylight Time Rule. 16
4.5.3 Configure the Date. 16
4.6 SNTP 16
5.0 SECURITY FEATURES 17
5.1 Manager and Operator passwords: 17
5.2 Console access interface and the CLI. 17
5.2.1 Manager 17
5.2.2 Operator 17
5.3 To use password security: 17
5.4 CLI: Setting Manager and Operator Passwords 17
5.4.1 Configuring Manager and Operator Passwords 17
5.5 Access Levels 17
5.6 Configuring and Monitoring Port Security 18
5.6.1 Basic Operation 18
5.6.2 Blocking Unauthorized Traffic 18
5.6.3 Planning For Port Security 18
5.7.1 Configuring Port Security 18
5.8 Reading Intrusion Alerts and Resetting Alert Flags 20
5.8.1 Notice of Security Violations 20
5.8.2 How the Intrusion Log Operates 20
6.0 CONFIGURATION FOR NETWORK MANAGEMENT APPLICATIONS 22
6.1 Overview 22
6.2 BitView and HubView 22
6.3 SNMP Management Features 23
6.4 Configuring for SNMP Access to the Switch 23
6.5 CLI: Viewing and Configuring Community Names 23
6.5.1 Listing Community Names 23
6.6 Configuring Community Names and Values 23
6.6.1 Adding SNMP Communities in the Switch 23
6.6.2 Adding SNMP Traps in the Switch 23
6.7 Using the CLI To List Current SNMP Trap Receivers 24
6.8 RMON 24
6.8.1 Adding RMON Communities in the Switch 24

7.0 MONITORING AND ANALYZING SWITCH OPERATION 25
7.1 Overview 25
7.2 CLI Access 25
7.3 Port Monitoring (Mirroring) Features 25
7.3.1 CLI: Configuring Port Monitoring 25
8.0 OPTIMIZING PORT USAGE 26
8.1 Overview 26
8.2 CLI: Viewing Port Status and Configuring Port Parameters 26
8.2.1 Port Status and Configuration Features 26
8.2.2 Port Status and Configuration Commands 27
8.2.3 Using the CLI to View Port Status 27
8.2.4 Using the CLI To Configure Ports 28
9.0 PORT-BASED VIRTUAL LANS (STATIC VLANS) 29
9.1 General Use and Operation. 29
9.2 VLAN Support and the Default VLAN 29
9.3 General Steps for Using VLANs 29
9.4 CLI: Configuring VLAN Parameters 29
9.4.1 Displaying the Switch's VLAN Configuration. 30
9.4.2 Displaying the Configuration for a Particular VLAN 30
9.5 Creating a New Static VLAN 30
9.5.1 Changing the VLAN Context Level 30
9.6 Effect of VLANs on Other Switch Features 31
9.6.1 VLAN Restrictions 31
10.0 TROUBLESHOOTING 32
10.1 Overview 32
10.2 Troubleshooting Approaches 32
10.3 Console Access Problems 32
10.4 Unusual Network Activity 32
10.5 General Problems 33
10.5.1 Duplicate IP Addresses 33
10.5.2 SNTP or Gateway Problems 33
10.6 Using the Event Log To Identify Problem Sources 33
10.7 Diagnostic Tools 36
10.7.1 Ping Test 36
10.7.2 CLI: Ping Test 36
10.8 CLI Administrative and Troubleshooting Commands 36
APPENDIX A 37
APPENDIX B 38

1.0 GETTING STARTED

1.1 Getting Started with Switch Configuration

This section is a guide for using the console Switch Setup commands to quickly assign an IP (Internet Protocol) address and subnet mask to the switch. You can also set a Manager password and configure other basic features from Switch Setup commands.

For Hardware Installation and configuration, please see the user guide for hardware.

1.2 Software Upgrade

If your Magnum 6K already has the software then you will get the Login prompt when you boot up the switch, otherwise you will get the Boot prompt and you will have to upgrade the software (For details refer Appendix D)

Below is a screen example of the boot prompt.

```
Copyright (c) 2001 GarrettCom Inc All rights reserved.

RESTRICTED RIGHTS
-----------------

Use, duplication or disclosure is subject to U.S. Government restrictions
as set forth in Sub-division (b)(3)(ii) of the rights in Technical Data and
Computer Software clause at 52.227-7013.

   GarrettCom, Inc.
   213, Hammond Avenue,
   Fremont,
   CA 94539,
   United States (USA)
   www.garrettcom.com

Magnum6K25(boot) build Nov  8 2001,21:30:49
MAC Address: 00:20:06:25:00:0E

Magnum6K25(boot)#
```

1.3 Recommended Minimal Configuration

In the factory default configuration, the switch has no IP (Internet Protocol) address and subnet mask. In this state, it can be managed only through a direct console connection. To manage the switch through in-band (networked) access, you should configure the switch with an IP address and subnet mask compatible with your network. Also, you should change the Manager password to control access privileges from the console. The default password is “manager” for the Manager user and “operator” for the Operator user respectively. Many other features such as optimizing the switch’s performance, enhancing your control of the network traffic, and improving network security can be configured through the switch’s console interface. Once an IP address has been configured on the switch, these features can be accessed more conveniently through an SNMP network management station running a network management program. For a listing of switch features available with and without an IP address, refer to Chapter: “How IP Configuration”.

1.4 Using the Console Setup Screen

The quickest and easiest way to minimally configure the switch for management and password protection in your network is to use the following sequence. Use a direct console connection to the switch, start a console session, and access the Switch Setup screen.

1. Using the method described in the preceding section, connect a terminal device to the switch and it will display the switch console command (CLI) prompt (the default display).

The CLI prompt appears displaying the switch model number:
Magnum6K25#

Below is an example of the above prompt.

```
Copyright (c) 2001 GarrettCom, Inc. All rights reserved.

RESTRICTED RIGHTS
-----------------
Use, duplication or disclosure  is subject to  U.S. Government restrictions
as set forth in Sub-division (b)(3)(ii) of the rights in Technical Data and
Computer Software clause at 52.227-7013.

    GarrettCom, Inc.
    213, Hammond Avenue,
    Fremont,
    CA 94539,
    United States (USA)
    www.garrettcom.com
Magnum6K25 build Jan 14 2002,12:12:53

login:manager
password:*******
Magnum6K25#
Magnum6K25#
```

Below is the sequence of activities that must be completed for the network to find your switch.

2. Set the **Manager Password** (optional).
3. Configure the **IP Address** and enter the IP address that is compatible with your network.
4. Configure the **Subnet Mask** and enter the subnet mask used for your network.
5. Configure the **Default Gateway** of your Network.

Syntax: ipconfig ip=<ipaddress> mask=<subnet mask> dgw=<default-gateway>
Example: **ipconfig ip=192.168.1.150 mask=255.255.255.0 dgw=192.168.1.10**

6. Restart the unit.

The switch is now configured with a Manager password, IP address, and subnet mask, and can be accessed through the Console or an SNMP-based network management tools. Here is some information about the basic fields.

Parameter	**Default**	
System Name	blank	Optional;
System Contact	blank	Optional;
Manager Password	manager	Recommended;
Logon Default	CLI	The default setting .
Time Zone	0 (none)	Optional;
Community Name	public	Default setting recommended.
Default Gateway	blank	Optional
IP Address	xxx.xxx.xxx.xxx	Recommended;

Note: The IP address and subnet mask assigned for the switch must be compatible with the IP addresses used in your network. For more information on IP addressing, see the *Chapter 3.*

1.5 To Recover from a Lost Manager Password:

If you cannot start a console session at the manager level because of a lost Manager password, Please contact support@garrettcom.com.

2.0 Console Management Interface

This chapter describes the following:

?? Management interfaces for the Magnum Switch 6K25.
?? Advantages of using CLI interface.

2.1 Understanding Management Interfaces

The console interface is accessed through the DB-9 RS232 connector. Attach a VT100 compatible terminalor a PC running a terminal emulation program to the serial port.

Management interfaces enable you to reconfigure the switch and to monitor switch status and performance. The Magnum switch 6K25 offers the CLI interface:

?? CLI – A command line interface offering the full set of switch commands through the VT-100 or equivalent console built into the switch.

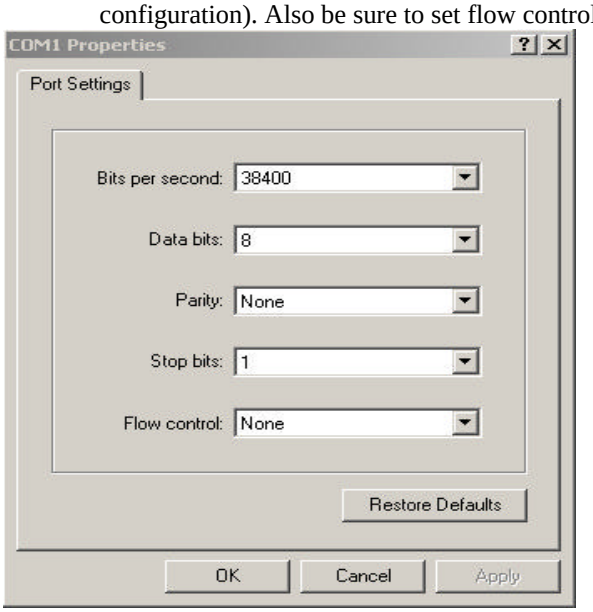
This manual describes how to use the CLI and how to use these interfaces to configure and monitor the switch.

The MNS software supports a command-line interface (CLI) through the serial port.
Note: In Release 2 the CLI will also be accessible through Telnet.
The command-line interface enables local or remote unit installation and maintenance. A set of system commands allows effective monitoring, configuration and debugging of the device.

2.2 Console Port Connection

Attach a VT100 compatible terminal or a PC running a terminal emulation program to the serial port on the switch. Use the null-modem cable.

When attaching to a PC, set terminal emulation type to VT100, specify the port used by your PC (i.e, COM 1~4), and then set communications to 8 data bits, 1 stop bit, no parity, and 38400 bps (for initial configuration). Also be sure to set flow control to 'none'.



2.3 Advantages of Using the CLI

Magnum6K25>	Operator Level
Magnum6K25#	Manager Level
Magnum6K25##	Configuration Level

?? Provides access to the complete set of switch configuration, performance, and diagnostic features.

?? Enables quick management level access of the detailed system configuration to system operators and administrators experienced in command prompt interfaces.

?? Provides help at each level for determining available options and variables.

2.4 CLI Usage

?? To perform specific procedures such as configuring IP addressing or VLAN.

?? To monitor and analyze switch operations.

?? For more information on individual CLI commands, refer to the Index or to the “Command Line Interface Reference Guide” available on GarrettCom’s web site.

3.0 Using the Command Line Interface (CLI)

The **CLI (Command Line Interface)** is a text-based command interface for configuring and monitoring the switch. The CLI gives you access to the switch's full set of commands while providing password protection.

The switch executes a multi-tasking operating system on its control processor that manages all system activities. This system allows the administrator to query and configure the switch from either an attached terminal or any of its attached network interfaces.

3.1 Accessing the CLI

This section provides information on how to access the console commands and set or enable the advanced configuration features in the switch.

The CLI is accessed through the switch console. You can access the console out-of-band by directly connecting a terminal device to the switch, or in-band by using Telnet **(R2)** either from a terminal device or through the network interface.

3.2 Using the CLI

The CLI offers the following privilege levels to prevent unauthorized access to the switch:

Operator
Manager

When you use the CLI mode to make a configuration change, the switch writes the changes to the Running Configuration file in volatile memory. This allows you to test your configuration changes before making them permanent. To make changes permanent, you must use the **save** command to save them to the Startup Configuration file in non-volatile memory. If you reboot the switch without first using **save**, all changes made since the last reboot or **save** (whichever is later) will be lost.

3.3 Privilege Levels at Logon

Privilege levels control the type of access to the CLI. To implement this control, you must set the Manager password (By default, the manager password is "manager". If passwords are set when you use the CLI to log on to the switch, you will be prompted to enter a user then enter a password.

For example:

```
Copyright (c) 2001 GarrettCom, Inc. All rights reserved.
RESTRICTED RIGHTS
Use, duplication or disclosure is subject to U.S. Government restrictions
as set forth in Sub-division (b)(3)(ii) of the rights in Technical Data and
Computer Software clause at 52.227-7013.

   GarrettCom, Inc.
   213, Hammond Avenue,
   Fremont,
   CA 94539,
   United States (USA)
   www.garrettcom.com
Magnum6K25 build Jan 14 2002,12:12:53

login:
```

3.3.a Example of CLI Login Screen

In the above case, you will enter the CLI at the level corresponding to the user and password combination you provide (operator or manager). Suppose you log onto the CLI at the Manager level, the following prompt will appear:
Magnum6K25#_

We strongly recommend that you change both the Manager and the operator password. Note that changing only an Operator password *does not* prevent access to the Manager level by intruders who have the Manager password.

Operator Privileges

At the Operator level you can examine the current configuration and move between interfaces without being able to change the configuration. A ">" character delimits the Operator-level prompt.

For example:

Magnum6K25>_ (Example of the Operator prompt.)

Manager Privileges
Manager privileges give you an additional level of access: A "#" character delimits any Manager prompt.
For example:

Magnum6K25#_ (Example of the Manager prompt.)

The above prompt provides all Operator level privileges plus the ability to perform system-level actions that do not require saving changes to the system configuration file. The prompt for the Manager level contains only the system name and the "#" delimiter, as shown above. To go to configuration mode, enter the **configure** command. You will get the "##" delimiter, as shown below.

Magnum6K25# **configure vlan type=port**
Magnum6K25(vlan-port)##_ (The Configuration Prompt)

3.4 Listing Commands and Command Options

At any privilege level you can:

- ?? List all of the commands available at that level
- ?? List the options for a specific command

Listing Commands Available at Any Privilege Level
At a given privilege level you can execute the commands that level offers plus all of the commands available at preceding levels. For example, at the Operator level you can list and execute only the Operator level commands. However, at the Manager level you can list and execute the commands available at both the Operator and Manager levels.
Privilege Level Example of Prompt and Permitted Operations

3.4.1 Operator Privilege

-View status and configuration information.
-Perform connectivity tests.
-Move from the Operator level to the Manager level using the '**enable**' command.
-Exit from the CLI interface and terminate the console session using the '**logout**' command.

For a list of available commands, enter 'help' at the prompt.
For example, to view status and configuration information of the Operator Level use the **show** command:
Magnum6K25> **show** <*command*>

3.4.2 Manager Privilege

At the Manager Level (Magnum6K25#) prompt you can perform system-level actions such as system control, configuration, monitoring, and diagnostic commands, plus any of the Operator-level commands. For a list of available commands, enter 'help' at the prompt.

At the Configuration (Magnum6K25##) prompt you can execute configuration commands, plus all Operator and Manager commands. For a list of available commands, enter 'help' at the Context Configuration prompt.

3.4.3 Type "help" To List Available Commands.

Typing the '**help**' command lists the commands you can execute at the current privilege level. For example, typing '**help**' at the Operator level produces this listing:

Magnum6K25> help

```
Magnum6K25> help
Command available in this (main) context

    exit     :Exits from the current configuration context
    logout   :Logs out from the console session
    show     :Displays the various configuration settings and parameters
    set      :Modifies various configuration settings and parameters
    enable   :Configures the operator to the manager mode
    clear    :Clears the Event Log or Command history
    ping     :To test the existense of remote host

For help on any command enter help <command>
For help on a specific configuration context enter help <context>
For command usage information, enter the command without parameter
```

Typing '**help**' at the Manager level produces this listing

Magnum6K25# help

```
Command available in this (main) context

    ipconfig :Configures the IP protocol parameters for switch
    upgrade  :Go to the system prompt to upgrade software
    exit     :Exits from the current configuration context
    logout   :Logs out from the console session
    show     :Displays the various configuration settings and parameters
    set      :Modifies various configuration settings and parameters
    enable   :Configures the operator to the manager mode
    clear    :Clears the Event Log or Command history
    reboot   :Reboots the system
    ping     :To test the existense of remote host
    configure:Go to a specified configuration context by syntax shown below
              vlan type=<type> :Configures VLANs of <type>
              rmon             :Configures the Rmon
              port-security    :Configures port security
              sntp             :Configures parameters for SNTP system
              snmp             :Configures parameters for SNMP system
              port-mirror      :Configures port mirroring
              device           :Configures devices

For help on any command enter help <command>
For help on a specific configuration context enter help <context>
--More--
```

3.4.4 Displaying CLI "Help"

CLI Help provides four types of context-sensitive information:

- ?? Command list with a brief summary of each command's purpose.
- ?? Detailed information on how to use individual commands.
- ?? Command line verbosity with possible options.
- ?? Command usage of specific commands.

3.4.5 Displaying Help for an Individual Command.

You can display Help for any command that is available at the current context level by typing help then entering enough of the command string to identify the command.

Syntax: **help** <*command string*>

For example, to list the Help for the **set time** command at the Configuration privilege level type:

Magnum6K25# **help set time**

```
Magnum6K25# help set time
Usage
    set time zone=<string> hour=<0-23> min=<0-59> sec=<0-59> format=<12|24>
             Sets the system time.The time zone must be entered as a string in
             the format GMT+HH:MM or GMT-HH:MM as appropriate for the country.
             Please consult the user manual for information on countries and
             time zones.
             If sntp is not used,the date and time need to be set every
             time the switch is powered up.
```

3.4.6 Displaying Help for a particular command.

You can display the command usage of a specific command by typing the command and pressing enter.

Syntax: **<Command Name> <Enter>**

```
Magnum6K25# show
Usage
    show ipconfig :Display the IP protocol parameters of the switch
    show version  :Display the current version of the software
    show port     :Display the port information
    show port-mirror:Display the port mirroring parameters
    show port-security:Display the port-security parameters
    show sntp     :Display the SNTP client parameters
    show snmp     :Display the SNMP protocol parameters
    show log      :Display the event log
    show date     :Display the current date and time
    show setup    :Display the current setup parameters of the system
    show history  :Display the previous command history
    show arp      :Display the ARP cache
    show rmon <stats|hist|event|alarm|defaults>:Display RMON data of speci-
                  fied type
    show vlan     :Display current VLAN type
    show vlan type=<port|tag|mac> : Display VLAN parameter of specified type
```

3.4.7 Displaying Help with all possibilities.

You can display Help for all possible commands and options that are available by pressing the <TAB> key.

Syntax: <TAB>

Or <Command string> <TAB>

Or <First character of the command> <TAB>

For example, <TAB> will list the available commands in the particular privilege level:

Magnum 6K25> **<TAB>**
exit
logout
show
set
help
enable
clear

Magnum 6K25> **s <TAB>**
show
set

Magnum 6K25# **set <TAB>**
password
daylight
time
date

4.0 Configuring IP Addressing, Interface Access, and System Information

4.1 IP Configuration

4.1.1 IP Address and Subnet Mask.

Configuring the switch with an IP address expands your ability to manage the switch and use its features. To configure IP addressing, use the menu interface (R2 only) or the CLI to manually configure the initial IP values.

4.1.2 Default Gateway Operation.

The default gateway is required when a router is needed for tasks such as reaching off-subnet destinations or forwarding traffic across multiple VLANs. The gateway value is the IP address of the next-hop gateway node for the switch, which is used if the requested destination address is not on a local subnet/VLAN.

4.2 A Quick Start

If you just want to give the switch an IP address so that it can communicate on your network, or if you are not using VLANs, GarrettCom recommends that you use the CLI commands to quickly configure IP addressing. To do so, do one of the following:

Enter the following command at the CLI Manager level prompt.
Magnum6K25# **ipconfig ip** = <ipaddress> **mask** = <subnet-mask>
dgw= <default-gateway>

Syntax: **show ipconfig**
For example, in the factory-default configuration (no IP addressing assigned) the switch's IP addressing appears as:

Magnum6K25> **show ipconfig**
IP Address : 192.168.1.25
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.10

4.3 Interface Access: Console/Serial Link, Features

In most cases, the default configuration is acceptable for standard operation.

Note Basic switch security is through passwords. You can gain additional security using IP authorized managers. However if unauthorized access is gained to the switch through in-band (Telnet), then you can disallow in-band access (as described in this section) and install the switch in a locked environment.

Feature	**Default**
Inactivity Time	0 Minutes(disabled)
Terminal Type	VT-100
Event Log event types to list (Displayed Events)	All
Baud Rate	38400
Flow Control	None

4.4 System Information

Configuring system information is optional, but recommended.

System Name: Using a unique name helps you to identify individual devices in stacking environments and when using SNMPc, HP Open View or any other NMS software for Hubs & Switches.

4.4.1 System Contact and Location:

This information is helpful for identifying the person administratively responsible for the switch and for identifying the locations of individual switches.

4.4.2 Time Zone:

The number of minutes your time zone location is to the West (+) or East (-) of Coordinated Universal Time (formerly GMT). The default **0** means no time zone is configured.

4.5 CLI: Listing the Current System Information.

4.5.1 List the current system information settings.

type: **show setup**

This example shows the switch's default console configuration.

```
Magnum6K25# show setup
MAC Address      : 00:11:21:30:40:50
IP Address       : 192.168.1.150
Subnet Mask      : 255.255.255.0
Default Gateway  : 192.168.1.1
CLI Mode         : Manager
Timezone         : GMT-08:00
sysName          : Magnum6K25
sysDescr         : 25 Port Modular Ethernet Switch
sysContact       : support@garrettcom.com
sysLocation      : Fremont, CA, USA
sysObjectID      : 1.3.6.1.4.1.553.12.6
```

4.5.2 Configure the Time Zone and Daylight Time Rule.

These commands:

?? Set the time zone you want to use

?? Define the daylight time rule for keeping the correct time when daylight-saving-time shifts occur.

Syntax: **set time zone**=<string> **hour**=<0-23> **min**=<0-59> **sec**=<0-59> **format**=<12|24>

set daylight country=<string>

4.5.3 Configure the Date.

The switch uses the date command to configure the date. Note that the CLI uses either a 12 or 24-hour clock scheme; that is, hour *(hh)* values from 1 p.m. to midnight are input either as 1 or 13. You can set the format with the help of the **set time** command.

Syntax: **set date year**=<2000-2036> **month**=<1-12> **day**=<1-31> **format**=<ddmmyyyy|mmddyyyy|yyyymmdd>

For example, to set the switch to 3:45 p.m. on October 1, 2001 in California USA input "GMT – 08:00" :

Magnum6K25## **set time zone**= GMT-08:00 **hour**=15 **min**=45 **sec**=0 **format**=12

Magnum6K25## **set date year**=2001 **month**=10 day=1 **format**=mmddyyy

Note: Executing **reboot** resets the time and date to their default startup values.

4.6 SNTP

Simple Network Time Protocol

The SNTP protocol is used to allow network access to accurate clocks and other sources of time base information that is an adaptation of the Network Time Protocol (NTP) used to synchronize device clocks in the Internet.

The SNTP client of the Magnum 6K25 has the ability to set the SNTP server IP address. The SNTP client synchronizes the time and date with the SNTP server.

CLI Commands

Syntax: Magnum6K25# **setsntp server** = <ipaddress> **timeout** = <1-10> **retry** = <1-3>

E.g., Magnum6K25# **setsntp server = 204.65.129.201 timeout = 3 retry = 3**

Once the IP address of SNTP assigned then enable the SNTP service.

Syntax: Magnum6K25# **sntp** <enable|disable>

5.0 Security Features

5.1 Manager and Operator passwords:

You can gain access and privileges for the command line and menu interfaces **(R2)** through either the console port or through the network by using Telnet **(R2)**. The features described in this chapter enhance security controls against unauthorized access through the network.

5.2 Console access interface and the CLI.

There are two levels of console access: *Manager* and *Operator*. For security, you can set a password on each of these levels.

5.2.1 Manager

This level allows access to all console interface areas.

Please change the default Manager Password to limit access of unauthorized people to the configuration area of the console interface.

5.2.2 Operator

This level allows access to the Status, Event Log, and CLI levels but does not allow Configuration capabilities. On the Operator level, the Configuration Context, Download Application, and Reboot Switch option are not accessible.

5.3 To use password security:

1.Set a Manager password (and an Operator password, if applicable for your system).

2.Exit from the current console session. A Manager password will now be needed for full access to the console.

Assuming that both a Manager password and an Operator password have been set, the level of access to the console interface will be determined by which password is entered in response to the prompt. The manager and operator passwords control access to the menu interface **(R2),** and the CLI.
Note: Passwords are case-sensitive.

5.4 CLI: Setting Manager and Operator Passwords

5.4.1 Configuring Manager and Operator Passwords

This procedure prompts you to enter a password twice to help verify that you have correctly entered the desired characters.

Syntax: ***set*** **password**

Magnum6K25# **set password**
Enter old password:********
Enter new password:*********
Confirm password :*********
Password changed successfully
Note: Password must be 4-10 characters

5.5 Access Levels

For each authorized user, the Manager & Operator have specific access levels (For Details, Please see *Chapter 2*).

5.6 Configuring and Monitoring Port Security

The port security feature can be used to block input to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC (Media Control Address) of the station attempting to access the port is different from any of the MAC addresses specified for that port. In the event of security violation, the port can be configured to go into the disable mode or drop mode. The drop mode allows the user to configure the port to remain enabled during a security violation and drop only packets that are coming in from insecure hosts.

5.6.1 Basic Operation

Default Port Security Operation: The default port security setting for each port is off. That is, any device can access a port without causing a security reaction.

Intruder Protection: A port that detects an " intruder" blocks the intruding device or drops the packets from transmitting to the network through that port.

General Operation for Port Security: On a per-port basis, you can set up security measures to block unauthorized devices and send notice of security violations. Once you have configured port security, you can then monitor the network for security violations through the Event Log.

For any port, you can configure the following:

Authorized (MAC) Addresses: Specify devices (MAC addresses) that are allowed to send inbound traffic through the port.

This feature:

• Closes the port to inbound traffic from any unauthorized devices that are connected to the port.

• Provides the option for sending information to the log of a detected attempted security violation to a network management station and disables the port.

Note: There is a limitation of 10 MAC addresses per port for Port Security. The more MAC addresses programmed, the larger the burden on the CPU.

5.6.2 Blocking Unauthorized Traffic

Unless you configure the switch to disable a port or drop the packets when a security violation is detected, the switch security only blocks unauthorized traffic without disabling the port. This feature enables you toapply the security configuration to ports on which hubs, switches, or other devices are connected and maintain security while also maintaining network access to authorized users.

5.6.3 Planning For Port Security

1.Plan your port security configuration and monitoring according to the following:

a. On which ports do you want to configure port security?

b. Which devices (MAC addresses) are authorized on each port?

c. For each port, what security actions do you want? (The switch automatically blocks intruders detected on that port from transmitting to the network.) The switch can be configured to (i) Send intrusion alarms to the event Log and (ii) optionally disable the port on which the intrusion was detected.

d. How do you want to learn of the security violation attempts the switch detects? You can use the Event Log (through the CLI **show log** command) to see the intrusion.

2. Use the CLI commands to configure port security operating and address controls.

5.7 CLI: Port Security Command Options and Operation

5.7.1 Configuring Port Security

Syntax: **configure port-security**

Magnum6K25# **configure port-security**

It will take you to the configuration mode to configure the port security.

Adding an Authorized Device to a Port.
Syntax: **allow macs** <addresses> **port** = <number>
To simply add a device (MAC address) to a port's existing Authorized Addresses list, enter the port number with the **mac-address** parameter and the device's MAC address.

Magnum6K25(port-security)## **allow macs 00:c1:00:7f:ec: 00 00:60:b0:88:9e:00 port = 18**
In above example, two authorized devices are allowed for port number 18.

To See the Authorized Devices
Syntax: **show port-security**
Magnum6K25# **show port-security port=18**
After executing the above command, the security configuration for port 18 would be:
Port :18
Action :Disable
Signal :Log
Learn Mode :Enable
MAC_Addresses: 00:c1:00:7f:ec:00 00:60:b0:88:9e:00

To see all the Ports,
Magnum6K25# **show port-security**
Status: Port-security Disabled

Port	Action	Signal	Learn_Mode	Mac_Address
1	None	None	Disable	None
2	None	None	Disable	None
3	None	None	Disable	None
4	None	None	Disable	None
5	None	None	Disable	None
6	None	None	Disable	None
7	None	None	Disable	None
8	None	None	Disable	None
9	None	None	Disable	None
10	None	None	Disable	None
11	None	None	Disable	None
12	None	None	Disable	None
13	None	None	Disable	None
14	None	None	Disable	None
15	None	None	Disable	None
16	None	None	Disable	None
17	Drop	Log	Enable	None
18	Drop	Log	Enable	00:c1:00:7f:ec:00 00:60:b0:88:9e:00
19	Drop	Log	Enable	None
20	Drop	Log	Enable	None
21	Drop	Log	Enable	None
22	Drop	Log	Enable	None
23	Disable	Log	Enable	00:e0:29:6c:a4:fd
24	Drop	Log	Enable	None
25	None	None	Disable	None

Ports can also learn the MAC addresses with the help of the following command.
Syntax: **learn port=<number-list> <enable|disable>**
Magnum6K25(port-security)## **learn port=17,18 enable**
In the above example, Port 17 and 18 start learn the MAC addresses of connected devices.

Removing a Device From the " Authorized" List for a Port.

This command option removes unwanted devices (MAC addresses) from the Authorized Addresses list. (An Authorized Address list is available for each port where Learn Mode is set to " Static"

To use the CLI to remove a device that is no longer authorized:

Example: suppose port 18 is configured as shown below and you want to remove 00c100-123456 from the Authorized Address list:

Magnum6K25# **show port-security port=18**
Port :18
Action :Disable
Signal :Log
Learn Mode :Disable
MAC_Addresses: 00:c1:00:7f:ec:00 00:60:b0:88:9e:00

The following command serves this purpose by removing
00:c1:00:7f:ec:00

Magnum6K25(port-security)## **remove mac 00:c1:00:7f:ec:00 port 18**

The above command sequence results in the following configuration for port 18:

Magnum6K25# **show port-security port=18**
Port :18
Action :Disable
Signal :Log
Learn Mode :Disable
MAC_Addresses:00:60:b0:88:9e:00

5.8 Reading Intrusion Alerts and Resetting Alert Flags

5.8.1 Notice of Security Violations

When the switch detects an intrusion on a port, it sets an " alert flag" for that port and makes the intrusion information available as described below. When a security violation occurs on a port configured for Port Security, the switch logs the intruder activity in the event log.

– The show log command displays the Intrusion Log and the Event Log with different options.

5.8.2 How the Intrusion Log Operates

When the switch detects an intrusion attempt on a port, it enters a record of this event in the event Log. The event Log lists the most recently detected security violation attempts. This gives you a history of past intrusion attempts also.

Example:

S Date Time Log Description
A 01-01-2001 12:05:52 AM PS:INTRUDER 00:e0:29:6c:a4:fd@port19, packet dropped
A 01-01-2001 12:07:04 AM PS:INTRUDER 00:50:0f:02:33:b6@port17, packet dropped
A 01-01-2001 12:07:16 AM PS:INTRUDER 00:e0:29:2a:f0:3a@port17, packet dropped
A 01-01-2001 12:07:16 AM PS:INTRUDER 00:01:03:e2:27:89@port17, packet dropped
A 01-01-2001 12:07:30 AM PS:INTRUDER 00:e0:29:08:d7:e9@port17, packet dropped
A 01-01-2001 12:07:32 AM PS:INTRUDER 00:10:dc:6e:52:95@port17, packet dropped
A 01-01-2001 12:07:34 AM PS:INTRUDER 00:e0:29:08:d6:43@port17, packet dropped

The above is an example of Multiple Intrusion Log Entries for the Same Port

The log shows the most recent intrusion at the top of the listing. Instead, if the log is filled when the switch detects a new intrusion, the oldest entry is dropped off the listing and the newest entry appears at the top of the listing.

5.8.3 CLI: Checking for Intrusions, Listing Intrusion Alerts

The following commands display port status including, whether there are intrusion alerts for any port(s), a list of the intrusions, and which specific ports had the intrusions.

Magnum6K25# **show log**

S Date Time Log Description

A 01-01-2001 12:05:18 AM PS:INTRUDER 00:50:0f:02:33:b6@port17, packet dropped
A 01-01-2001 12:05:26 AM PS:INTRUDER 00:02:b3:1d:05:dc@port17, packet dropped
A 01-01-2001 12:05:36 AM PS:INTRUDER 00:01:03:e2:27:89@port17, packet dropped
A 01-01-2001 12:05:40 AM PS:INTRUDER 00:e0:29:11:1b:af@port17, packet dropped
A 01-01-2001 12:05:44 AM PS:INTRUDER 00:02:b3:64:d8:cf@port17, packet dropped
A 01-01-2001 12:05:44 AM PS:INTRUDER 00:e0:29:09:5d:be@port17, packet dropped
A 01-01-2001 12:05:48 AM PS:INTRUDER 00:02:b3:08:d2:22@port17, packet dropped
A 01-01-2001 12:05:48 AM PS:INTRUDER 00:e0:29:2a:f0:3a@port17, packet dropped
A 01-01-2001 12:05:56 AM PS:INTRUDER 00:10:dc:40:57:95@port17, packet dropped
A 01-01-2001 12:06:02 AM PS:port 18 disabled, INTRUDER 00:e0:29:2a:f1:bd

This log shows the intrusion at the port 17 and 18. You can always clear the log with clear command.

Magnum6K25# **clear log**

It clears the complete log.

You can also clear the specific part of the Log.

Syntax: **clear log <informational|debug|activity|critical|fatal>**

Magnum6K25# **clear log activity**

It clears the ‘activity’ log only.

6.0 Configuration for Network Management Applications (SNMP)

This chapter includes:

- ??An overview of SNMP management for the switch
- ?Bitview and Hubview through SNMPc.
- ??Configuring the Series 6K switch for:
  - SNMP management
  - SNMP Communities
  - Traps Configuration
- ??Information on advanced management through RMON

To implement SNMP management, you must configure the switch with an appropriate IP address.

6.1 Overview

You can manage the switch via SNMP from a network management station.

For this purpose, GarrettCom recommends the **SNMPc**, an easy-to-install and use network management platform that runs on Windows based PC's. It uses the SNMP and RMON agents statistical sampling software that is included in the switch to provide powerful, but easy-to-use traffic monitoring and network activity analysis tools.

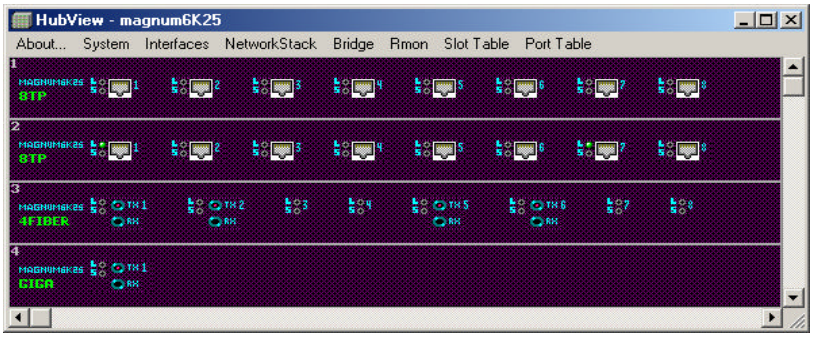
6.2 BitView and HubView

The BitView and HubView can be seen through SNMPc (Management PC Software).

Magnum6K25's that have BitView and HubView definitions can be managed graphically. BitView displays a bitmap image that matches the faceplate of the device, whereas HubView is a more generic view that shows the layout of the device, but always uses the same picture elements

BitView is functionally similar to HubView, but displays a more realistic image of supported devices. Generally, all the LEDs and other graphical elements available on the device front panel can be displayed with BitView. As with HubView, you can select a device slot or port, and then a menu to operate on the selected item.

Magnum6K25: Bitview



Magnum6K25: Hubview

6.3 SNMP Management Features

SNMP management features on the switch include:

SNMP version 1
Security via configuration of SNMP communities
Event reporting via SNMP
Managing the switch with an SNMP network management tool Supported *Standard* MIBs include:
• SNMP MIB-II (RFC 1213)
• Bridge MIB (RFC 1493)
ifGeneralGroup, ifRcvAddressGroup, ifStackGroup
• RMON MIB (RFC 1757)
• RMON: groups 1, 2, 3, and 9
(Statistics, Events, Alarms, and History)
• Version 1 traps (Warm Start, Cold Start, Link Up, Link Down, Authentication Failure, Rising Alarm, Falling Alarm)

• *GarrettCom Proprietary* MIB

6.4 Configuring for SNMP Access to the Switch

SNMP access requires an IP address and subnet mask configured on the switch. In other words, Network stacks should be configured with an IP address and subnet mask. Once an IP address has been configured, we can follow the same steps as configuring the CLI (see CLI section 6.5) to configure the SNMP Access.

To configure and add the appropriate traps please see the CLI section of this chapter.

6.5 CLI: Viewing and Configuring Community Names

Listing Current Community Names and Values

6.5.1 Listing Community Names

This command lists the data for currently configured SNMP community names.

Syntax: **show snmp <*community*|*traps*>**
Magnum6K25# **show snmp**
This example lists the data for all communities in a switch; that is, both the default "public" community name and another community named "private".
The configured community values are
Read Public
Write Private
Trap netman
Traps not configured

6.6 Configuring Community Names and Values

If you do not specify restricted or unrestricted for the read/write MIB access, the switch automatically restricts the community to read access for the MIB.

6.6.1 Adding SNMP Communities in the Switch

The following SNMP command add *new* SNMP communities:

Syntax: community [write=<string>] [read=<string>] [trap=<string>]
Magnum6K25(snmp)## **community write="private" read="public" trap="netman"**

6.6.2 Adding SNMP Traps in the Switch

The following SNMP command adds a new SNMP Trap:

Syntax: **traps add type=rmon|snmp|rmon,snmp|snmp,rmon|all ipaddress=<ipaddr>**
Magnum6K25(snmp)## **traps add type=all ipaddress=192.168.1.2**

6.7 Using the CLI To List Current SNMP Trap Receivers

This command lists the currently configured trap receivers along with the current SNMP community name data.

Syntax: **show snmp**

In the next example, the **show snmp** command shows that the switch has been previously configured to send SNMP traps to management stations belonging to the "public" and "private" communities.

Magnum6K25(snmp)## **show snmp**
The configured community values are
Read public
Write private
Trap netman
Traps are configured in the following way

Host	Traps
192.168.1.20	all

6.8 RMON

The switch supports RMON (Remote Monitoring) on all connected network segments. This allows for troubleshooting and optimizing your network.

The Magnum 6K25 switch provides hardware-based RMON counters in the switch chipset. The switch manager CPU polls these counters periodically to collect the statistics in a format that compiles with the RMON MIB definition.

The following RMON groups are supported:

- ?? Ethernet Statistics Group - maintains utilization and error statistics for the switch port being monitored.
- ?? History Group – gathers and stores periodic statistical samples from previous Statistics Group.
- ?? Alarm Group – allows a network administrator to define alarm thresholds for any MIB variable.
- ?? Log and Event Group – allows a network administrator to define actions based on alarms. SNMP Traps are generated when RMON Alarms are triggered.

The RMON agent automatically runs in the switch. Use the RMON management station on your network to enable or disable specific RMON traps and events.

6.8.1 Adding RMON Communities in the Switch

The following RMON commands add *new RMON* communities:

history def-owner = <string>
statistics def-owner = <string>
alarm def-owner = <string>
event def-owner = <string>
e.g.,
Magnum6K25(rmon)## **event def-owner = "test"**
The **show** command lists the RMON data of specified type.
Syntax: **show rmon <stats|hist|event|alarm>**
Magnum6K25# show rmon stats

IFS	STATUS
1	Valid
2	Valid
3	Valid
.	
.	
.	
24	Valid
25	Valid

7.0 Monitoring and Analyzing Switch Operation

7.1 Overview

The Magnum 6K25 Switches have several built-in tools for monitoring, analyzing, and troubleshooting switch and network operations:

Status: Includes options for displaying general Switch information, management address data, and MAC addresses.
Event Log: Lists Switch operating events and Alert events.
Configurable trap receivers: Uses SNMP to enable management stations on your network to receive SNMP traps from the Switch.
Port monitoring (mirroring): Copies all traffic from the specified ports to a designated monitoring port.

7.2 CLI Access

Syntax: **show setup**

```
Magnum6K25# show setup
Version          : Magnum6K25_build_Mar 22 2002,00:24:46 [A.01.023]
MAC Address      : 00:20:06:25:00:09
IP Address       : 192.168.1.150
Subnet Mask      : 255.255.255.0
Default Gateway  : 192.168.1.1
CLI Mode         : Manager
Timezone         : GMT+00:00 Daylight NONE
sysName          : Magnum6K25
sysDescr         : 25 Port Modular Ethernet Switch
sysContact       : support@garrettcom.com
sysLocation      : Fremont, CA, USA
sysObjectID      : 1.3.6.1.4.1.553.12.6
```

7.3 Port Monitoring (Mirroring) Features

You can designate a port for monitoring traffic of one or more ports on the Switch. The Switch monitors the network activity by copying all traffic from the specified monitoring sources (ports or VLAN) to the designated monitoring (mirror) port, to which a network analyzer can be attached.

7.3.1 CLI: Configuring Port Monitoring

You must use the following configuration sequence to configure port monitoring in the CLI:

1. Assign a monitoring (mirroring) port.
2. Designate the port to monitor.

To list the ports assigned to mirror (receive monitored traffic) and the ports being monitored you need to use the command below:
Syntax: **show port-mirror**
For example, if you assign port 12 as the monitoring port and configure the Switch to monitor port 3, **show port-mirror** displays the following:

Magnum 6K25> **show port-mirror**
Port mirroring is Enabled
Monitor Port is : 3
Sniffer Port is : 12
Configuring the monitor port assigns or removes a monitoring port. This must be executed from the configuration level. Removing the monitor port disables port monitoring and resets the monitoring parameters to their factory-default settings.
Syntax:
setport monitor=<number> sniffer=<number>
For example, to assign port 12 as the monitoring port and 3 as the monitored port, *type syntax*:
Magnum6K25## **setport monitor=3 sniffer=12**
To turn off port monitoring *type syntax*:
Magnum6K25# **prtmr disable**

8.0 Optimizing Port Usage

8.1 Overview

This chapter includes:

- ?? Configuring port, status, mode (speed and duplex), and flow control parameters.
- ?? Configuration screens corresponding to the port numbers on the front of the switch.

8.2 CLI: Viewing Port Status and Configuring Port Parameters

From the CLI commands, you can configure and view all port parameter settings and view all port status indicators.

8.2.1 Port Status and Configuration Features

Status or Parameter	Description
Status	**Enable** (default): The port is ready for a network connection. **Disable:** The port will not operate even when properly connected in a network. Use this setting if the port needs to be shut down for diagnostic purposes or while you are making topology changes.
Link	**Up**: The port senses a linkbeat. **Down**: The port is not enabled, has no cables connected, or is experiencing a network error. For troubleshooting information, see the installation manual you received with the switch. See also chapter 9, " Troubleshooting" (in this manual).
Mode	The port's speed and duplex (data transfer operation) setting. **10/100Base-T ports**: • **Auto** (default): Senses speed and negotiates with the port at the other end of the link for data transfer operation (half-duplex or full-duplex). **Note:** Ensure that the device attached to the port is configured for the same setting that you selected here. Also, if " Auto" is used, the device to which the port is connected must operate in compliance with the IEEE 802.3u "Auto Negotiation" standard for 100Base-T networks. If the other device does not comply with the 802.3u standard, or is not set to "Auto", then the port configuration on the switch must be manually set to match the port configuration on the other device. To see what the switch negotiated for the Auto setting, use the CLI **show port** command. Possible port setting combinations for copper ports. ✍✍ 10HDx: 10 Mbps, Half-Duplex ✍✍ 10FDx: 10 Mbps, Full-Duplex ✍✍ 100HDx: 100 Mbps, Half-Duplex ✍✍ 100FDx: 100 Mbps, Full-Duplex Possible port settings for 100FX ports: ✍✍ 100FDx (default): 100 Mbps, Full-Duplex ✍✍ 100HDx: 100 Mbps, Half-Duplex Possible port settings for 10FL ports: ✍✍ 10HDx (default): 10 Mbps, Half-Duplex ✍✍ 10FDx: 10 Mbps, Full-Duplex **100/1000Base-T ports**:

• **Auto** (default): Senses speed and negotiates with the port at the other end of the link for port operation (MDI-X or MDI).
To see what the switch negotiated for the Auto setting, use the CLI **show port** command.
- ✍✍ 1000Fdx: 1000 Mbps (1Gbps), Full-Duplex only
- ✍✍ 100Fdx: 100 Mbps, Full-Duplex

Notes:
• To change the port speed on a transceiver port you are required to reboot the switch.
• Ensure that the device attached to the port is configured for the same setting that you selected here.
Also, if " Auto" is used, the device the port is connected to must also be configured to " Auto" and operate in compliance with the IEEE 802.3ab " Auto Negotiation" standard for 1000Base-T networks.

Gigabit fiber-optic ports (Gigabit-SX and Gigabit-LX):
- ✍✍ 1000FDx (default): 1000 Mbps (1 GBPS), Full Duplex only

• **Auto**: The port operates at 1000FDx and auto-negotiates flow control with the device connected to the port.

Flow Control

• **Disabled** (default): The port will not generate flow control packets and drops received flow control packets.
• **Enabled**: The port uses 802.3x Link Layer Flow Control, generates flow control packets, and processes received flow control packets.
With the port mode set to "Auto" (the default) and "Flow Control" set to enabled, the switch negotiates Flow Control on the indicated port. If the port mode is not set to "Auto", or if "Flow Control" is disabled on the port, then Flow Control is not used.

8.2.2 Port Status and Configuration Commands

From the CLI, you can configure and view all port parameter settings and all port status indicators.

8.2.3 Using the CLI to View Port Status

Use the following commands to display port status and configuration:

show port: Lists the full status and configuration for all ports on the switch.

Syntax: **show port**

```
Keys:E=Enable              D=Disable
     H=Half Duplex         F=Full Duplex
     NE=Port Donot Exist NA=Not Applicable
Port Name              Control Dplx Media  Link Speed Part Auto
1    A1                    E     H    10T   down  10    No   E
2    A2                    E     F    100Tx down  100   No   D
3    A3                    E     H    10T   down  10    No   E
4    A4                    E     H    10T   down  10    No   E
5    A5                    E     H    10T   down  10    No   E
6    A6                    E     H    10T   down  10    No   E
7    A7                    E     H    10T   down  10    No   E
8    A8                    E     H    10T   down  10    No   E
9    B1                    E     H    100Tx up    100   No   E
10   B2                    E     H    10T   down  10    No   E
11   B3                    E     H    10T   down  10    No   E
12   B4                    E     H    10T   down  10    No   E
13   B5                    E     H    10T   down  10    No   E
14   B6                    E     H    10T   down  10    No   E
15   B7                    E     H    10T   down  10    No   E
16   B8                    E     H    10T   down  10    No   E
17   C1                    E     H    10T   down  10    No   E
18   C2                    E     F    100Fx down  100   No   D
19   C3                    E     H    10T   down  10    No   E
--More--
```

show port=<Port number>: Lists the status of the specific port.

Syntax: **show port=2**

```
Magnum6K25# show port=2
Port Number       :2
Port Name         :A2
Control           :Enable
Status            :Enable
Duplex            :Full
Mediatype         :100Tx
Link Status       :down
Speed             :100
Partition         :No
Traffic           :0
AutoNegotiation   :Disable
```

8.2.4 Using the CLI To Configure Ports

You can configure one or more of the following port parameters. For details on each option, see Table above.

Syntax: **setport port**=<port-list> **status**=<enable|disable> **speed**=<10|100> **duplex**=<half|full> **auto**=<enable|disable>

For example, to configure ports 1 through 4 and port 7 for 100Mbps full-duplex, you would enter this command:
Note: Before changing the port setting, you have to 'disable' the auto- negotiation.

Magnum6K25(device)## **setport port=1- 4,7 speed=100 duplex=full**

Similarly, to configure a single port with the settings in the above command, you could enter the same command with only the one port identified.

Magnum6K25(device)## **setport port=7 speed=100 duplex=full**

If port 8 was disabled, and you wanted to enable it and configure it for 100FDx you could do so with the following command.

Magnum6K25(device)## **setport port=8 status=enable speed=100 duplex=full**

9.0 Port-Based Virtual LANs (Static VLANs)

A VLAN is a group of ports designated by the switch as belonging to the same broadcast domain. (That is, all ports carrying traffic for a particular subnet address would normally belong to the same VLAN.)

Note This section describes *static* VLANs, which are VLANs you manually configure with a name, VLAN ID (VID), and port assignments. Using a VLAN, you can group users by logical function instead of physical location. This helps to control bandwidth usage by allowing you to group high-bandwidth users on low-traffic segments and to organize users from different LAN segments according to their need for common resources.

By default, the Series 6K switches are VLAN (Port based) enabled and allow up to 32 port-based VLANs. The port-based nature of the configuration allows interoperation with older switches that require a separate port for each VLAN.

9.1 General Use and Operation.

Port-based VLANs are typically used to enable broadcast traffic reduction and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs that may be configured on a switch. Packets are forwarded only between ports that are designated for the same VLAN. Thus, all ports carrying traffic for a particular subnet address should be configured to the same VLAN. Cross-domain broadcast traffic in the switch is eliminated and bandwidth is saved by not allowing packets to flood out all ports. An external router is required to enable separate VLANs on a switch to communicate with each other.

9.2 VLAN Support and the Default VLAN

In the factory default configuration, VLAN support is enabled and all ports on the switch belong to the default VLAN (named DEFAULT-VLAN). This places all ports in the switch into one physical broadcast domain.

You can partition the switch into multiple virtual broadcast domains by adding one or more additional VLANs and moving ports from the default VLAN to the new VLANs. (The switch supports up to 32 VLANs.) You can change the name of the default VLAN, but you cannot change the default VLAN's VID (which is always " 1"). Although you can remove all ports from the default VLAN, this VLAN is always present.

To display the current VLAN, use the CLI **show vlan** command.
Syntax: **show vlan type=port**

9.3 General Steps for Using VLANs

1.Plan your VLAN strategy and create a map of the logical topology that will result from configuring VLANs. Include consideration for the interaction between VLANs .

2. Configure at least one VLAN in addition to the default VLAN.

3. Assign the desired switch ports to the new VLAN(s).

Notes on Using VLANs

- ?? You can rename the default VLAN, but you cannot change its VID (1) or delete it from the switch.
- ?? Any ports *not* specifically assigned to another VLAN will remain assigned to the DEFAULT-VLAN.
- ?? Changing the number of VLANs supported on the switch requires the SAVE command.

9.4 CLI: Configuring VLAN Parameters

In the factory default state, all ports on the switch belong to the default VLAN (DEFAULT-VLAN) and are in the same broadcast/multicast domain. You can configure up to 31 additional static VLANs by adding new VLAN names, and then assigning one or more ports to each VLAN.
(The switch accepts a maximum of 32 VLANs, including the default VLAN).

Steps:

- Go to Configuration mode

Syntax: **configure vlan type=port**

- Set default Vlan Type

Syntax: **setvlan type=port**

- Add VLAN

Syntax: **add vlan=<vid> name=<name> port=<port list>**

- Start Vlan

Syntax: **start vlan=<vid>**

- Save the configuration

Syntax: **save**

9.4.1 Displaying the Switch's VLAN Configuration.

The next command lists the VLANs currently running in the switch, with VID, VLAN name, and VLAN status.

Syntax: **show vlan**

Magnum6K25# **show vlan**

Current vlan is set to Port

Magnum6K25# **show vlan type=port**

NAME	ID	STATUS	PORT LIST
DEFAULT-VLAN	1	Enable	1,2,3,4,5,6,7,8,9,10
Engg-Vlan	2	Enable	11,12,13,14,15
Fin-Vlan	3	Enable	8,9,10,116,17,18

9.4.2 Displaying the Configuration for a Particular VLAN

This command uses the VID to identify and display the data for a specific static VLAN.

Syntax: **show vlan type=port name=<*vlan-name*>**

Magnum6K25# **show vlan type=port name="Engg-Vlan"**

NAME : Engg-Vlan
VLAN ID : 2
PORT LIST : 11,12,13,14,15
STATUS : Enable

9.5 Creating a New Static VLAN

9.5.1 Changing the VLAN Context Level.

With this command, entering a new VID creates a new static VLAN. Entering the VID or name of an existing static VLAN places you in the context level for that VLAN.

Syntax: **add id**=<number> **name**=<*name-str*> **port**=<number-list>

Creates a new static VLAN if a VLAN with that VID does not already exist, and places you in that VLAN's context level. If you do not use the name option, the switch uses " VLAN" and the new VID to automatically name the VLAN. If the VLAN already exists, the switch places you in the context level for that VLAN.

For example, to create a new static VLAN with a VID of 32:

Magnum6K25(vlan-port)## **add id=32 name="Mktg" port=10,11,12**

Port vlan added successfully

Magnum6K25# **show vlan type=port**

NAME	ID	STATUS	PORT LIST
DEFAULT-VLAN	1	Enable	1,2,3,4,5,6,7,8,9
Mktg	32	Disable	10,11,12

To enable the new VLAN type the following:

Magnum6K25(vlan-port)## **start vlan =<ID or port list>**

For example, Magnum6K25(vlan-port)## **start vlan = 32**

Resulting,

NAME	ID	STATUS	PORT LIST
DEFAULT-VLAN	1	Enable	1,2,3,4,5,6,7,8,9
Mktg	32	Enable	10,11,12

9.6 Effect of VLANs on Other Switch Features

9.6.1 VLAN Restrictions

?? A port must be a member of at least one VLAN. In the factory default configuration, all ports are assigned to the default VLAN (DEFAULT-VLAN; VID = 1).

?? Before you can delete a VLAN, you can optionally re-assign all ports in the VLAN to another VLAN. Ports that are members of other VLANs will retain these memberships while all other ports will fall back into the default VLAN.

10.0 Troubleshooting

10.1 Overview

This chapter addresses performance-related network problems that can be caused by topology, Switch configuration, and the effects of other devices or their configurations on Switch operation. (For Switch-specific information on hardware problems indicated by LED behavior, cabling requirements, and other potential hardware-related problems, refer to the Magnum 6K25 User Manual.)

This chapter includes:

?? Troubleshooting Approaches
?? Console Interface Problems
?? Unusual Network Activity
?? General Problems
?? VLAN-Related Problems
?? Using the Event Log To Identify Problem Sources
?? Diagnostics and Management Tools, including:
?? Ping test
?? Command prompt
?? Restoring the factory default configuration

For information on support and warranty provisions, see the Magnum 6K25 User Manual

10.2 Troubleshooting Approaches

Use these approaches to diagnose Switch problems:

?? Check the Switch LEDs for indications of proper Switch operation:
?? Each Switch port has a Link LED that should light whenever an active network device is connected to the port.

See the *Hardware User Guide* shipped with the Switch for a description of the LED behavior and information on using the LEDs for trouble-shooting.

?? Check the network topology/installation. See the *Hardware User Guide* shipped with the Switch for topology information.
?? Check cables for visible damage, correct type, and proper connections. See the *Hardware User Guide* shipped with the Switch for correct cable types and connector pin-outs.
?? For help in isolating problems, use the easy-to-access console port built into the Switch. See chapter 2, “Using the Console Interface” for operating information. These tools are available through the console port.

• Status and Counters screens
• Event Log
• Diagnostics tools (Ping test, and advanced user commands)

10.3 Console Access Problems

The Switch may not have the correct IP address, subnet mask, or gateway. Verify the problem by connecting a console to the Switch’s Console port and check the IP configuration.

10.4 Unusual Network Activity

Network activity that exceeds accepted norms may indicate a hardware problem with one or more of the network components, possibly including the Switch. Unusual network activity is indicated by the light patterns of the LEDs on the front of the Switch. This unusual activity can be measured with the Switch console interface or with a network management tool. Refer to the *Hardware User Guide* you received with the Switch for information on using LEDs to identify unusual network activity.

A topology loop can also cause excessive network activity. The event log messages can be indicative of this type of problem. Please see Using the Event Log To Identify Problem Sources section of this chapter for more detail.

10.5 General Problems

If you experience problems such as "the network runs slow; processes fail; or users cannot access servers or other devices" then Broadcast storms may be occurring in the network. These may be due to redundant links between nodes.

10.5.1 Duplicate IP Addresses

This is indicated by this Event Log message:

TCP/IP: duplicate IP Addresses [IP address] *sent from Ethernet address [*MAC address*]*.
The IP Address above is the same IP address of both devices, indicating the Switch's IP address has been duplicated somewhere on the network.

10.5.2 SNTP or Gateway Problems

If problems such as "The Switch Cannot Find the SNTP Server or the Configured Gateway" occur then your primary VLAN to the ports may have moved. SNTP and Gateway access are through the VLAN, which in the default configuration is the DEFAULT-VLAN. If the primary VLAN has been moved to another VLAN, it may be disabled or does not have ports assigned to it.

10.6 Using the Event Log To Identify Problem Sources

The Event Log records operating events as single-line entries listed in chronological order, and serves as a tool for isolating problems. Each Event Log entry is composed of four fields:

Severity Date Time Description

Severity is one of the following levels:
I (Information) indicates routine events.
A (Activity) indicates the activity on Switch.
D (Debug). reserved for Magnum internal diagnostic information.
C (Critical) indicates that a severe Switch error has occurred.
F (Fatal). indicates that a service has behaved unexpectedly.

Date is the date in *mm/dd/yy* format (as per configured) that the entry was placed in the log.
Time is the time in *hh:mm:ss* format (as per configured) that the entry was placed in the log.
Source Name is the name of the node, computer, device or the user.
Description is a brief description of the operating event.

The event log holds up to 1000 lines in chronological order, from the oldest to the newest. Each line consists of one complete event message. Once the log has received 1000 entries, it discards the current oldest line (with information level severity only) each time a new line is received. The event log window contains 22 log entry lines and can be positioned to any location in the log.
The event log is *not* erased by using the "Reboot Command" in the Main CLI.

CLI Command to see the Event Log
Type Syntax: **show log** <option>

```
-------------------------------------------------------------------------------------------
Severity   Date          Time                  Log   Description
-------------------------------------------------------------------------------------------
  D        21-09-2001  11:18:18 AM   System X   System is resetted
  I        21-09-2001  11:18:18 AM   Rajesh     Rajesh is now on line
  I        21-09-2001  11:18:18 AM   Server1    network enabled on  192.168.1.16
  A        22-09-2001   12:00:03PM   Device     Port 17 disabled
-------------------------------------------------------------------------------------------
```

The output can be filtered with the help of “Show Commands”.
E.g., *Type Syntax*: **show log informational** where “informational” is the <option> will show only informational log entries.

```
-------------------------------------------------------------------------------------------
Severity   Date          Time                  Log    Description
-------------------------------------------------------------------------------------------
   I       21-09-2001  11:18:18 AM   Rajesh      Rajesh is now on line
   I       21-09-2001  11:18:18 AM   Server1     network enabled on  192.168.1.16
```

Here is the List of System Events:

Subsystem	Description	Severity
SNTP	client started	I
SNTP	client stopped..disabled by user	I
SNTP	client stopped..server not configured	I
SNTP	Request timed out	I
SNTP	Retrying..	I
DEVICE	System started	I
DEVICE	Network Stack not yet configured	I
SNMP	Snmp.snmpEnableAuthenTraps is set to enabled	A
SNMP	Snmp.snmpEnableAuthenTraps is set to disabled	A
PRTMR	Enabled by user monitor = x , sniffer = y	I
PRTMR	Disabled by user	I
VLAN	Type set to port	I
VLAN	Type set to mac	I
VLAN	Type set to tag	I
VLAN	Type set to none	I
VLAN	Pvlan: port based vlan started	I
VLAN	Pvlan: default vlan is modified	I
VLAN	Tvlan: Tag based vlan started	I
TCP/IP	Failed to initialize the interface x	F
BRIDGE	Bridge init failed for ethx	F
BRIDGE	Bridge enable for ethx failed	F
DEVICE	IP address a.b.c.d configured	I
DEVICE	subnetmask a.b.c.d configured	I
DEVICE	Default gateway a.b.c.d configured	I
DEVICE	Switch rebooted by user	I
SNMP	System.sysName configured	A
SNMP	System.sysLocation configured	A
SNMP	System.sysContact configured	A
DEVICE	Port x enabled	A
DEVICE	Port x disabled	A
CLI	Manager login at console	I
CLI	Operator login at console	I
CLI	Manager password changed	I
CLI	Operator password changed	I
SNMP	read community string changed	I
SNMP	write community string changed	I
SNMP	trap community string changed	I
RMON	rising alarm trap sent to a.b.c.d by alarm entry X	I
RMON	falling alarm trap sent to a.b.c.d by alarm entry X	I
SNMP	authentication failure trap sent to a.b.c.d	I

SNMP	Trap receiver a.b.c.d added	I
SNMP	Trap receiver a.b.c.d deleted	I
DEVICE	No saved system logs	I
DEVICE	Failed to read saved system logs	D
SNMP	Coldstart trap sent to a.b.c.d	I
SNMP	Warmstart trap sent to a.b.c.d	I
SNMP	Port X link up trap sent to a.b.c.d	A
SNMP	Port X Link down trap sent to a.b.c.d	A
SNMP	Configuring IP address in trap receivers list failed	D
DEVICE	Timezone set to x	I
DEVICE	Country set to x (no DST)	I
DEVICE	Country set to x (DST valid)	I
DEVICE	Time set to x : y : z (HH:MM:SS) tz = a	I
DEVICE	Date set to x : y : z (HH:MM:YYYY)	I
RMON	RMON init is done	I
BRIDGE	Bridge MIB init is done	I
TCP/IP	Duplicate IP a.b.c.d sent from MAC address XXXXXX	C
TCP/IP	IP packet of version X is dropped	I
TCP/IP	IP packet from a.b.c.d , with checksum error dropped	D
TCP/IP	Bad IP fragments from a.b.c.d dropped	D
TCP/IP	UDP checksum error in the received packet a.b.c.d	D
TCP/IP	TCP checksum error in the received packet a.b.c.d	D
TCP/IP	Unable to allocate memory for an ICMP packet	C
TCP/IP	ICMP checksum error in the received packet	D
SNTP	Time synchronized through SNTP	I
RMON	history : control entry X is set to valid	I
RMON	history : control entry X is set to invalid	I
RMON	Event : entry X is set to valid	I
RMON	Event : entry X is set to invalid	I
RMON	Alarm : entry X is set to valid	I
RMON	Alarm : entry X is set to invalid	I
RMON	Alarm : internal error , unable to get memory	F
RMON	Alarm : internal error, unable to get memory for alarm entry	F
RMON	History : internal error, unable to get memory for history control entry	F
RMON	History : internal error, unable to get memory for history data entry	F
RMON	History : internal error, unable to get memory	F
RMON	Event : unable to get memory for event entry	F
RMON	Alarm : unable to get memory for RMON logs	F
DEVICE	Ethernet DMA init failure	F
DEVICE	Ethernet hardware error	F
DEVICE	Ethernet interrupt init failure	F
DEVICE	Ethernet counters init failure	C
BRIDGE	Unable to delete MAC address from FDB	D
BRIDGE	Unable to insert MAC address to FDB	D
DEVICE	Unable to access ethernet counters	C
DEVICE	Unable to allocate ethernet memory	F
DEVICE	Port X link down	A
DEVICE	Port X link up	A
PS	INTRUDER a:b:c:d:e:f @ port X , port disabled	A
PS	INTRUDER a:b:c:d:e:f @ port X , port disabled	A
PS	Resetting MAC a:b:c:d:e:f at port X failed	C

PS	Unable to delete learnt MACs in hardware	D
PS	Port security enabled	A
PS	port security disabled	A
VLAN	pvlan:vlan X enabled	I
VLAN	pvlan:vlan X disabled	I
VLAN	pvlan:vlan X deleted	I
VLAN	pvlan:port based VLAN started	I
VLAN	pvlan:port based VLAN stopped	I
VLAN	pvlan:default vlan is modified	I
VLAN	tvlan:vlan X deleted	I
VLAN	tvlan:vlan X enabled	I
VLAN	tvlan:vlan X disabled	I
VLAN	tvlan:tag based VLAN stopped	I
VLAN	tvlan:tag based VLAN started	I

10.7 Diagnostic Tools

10.7.1 Ping Test

The Ping test is a point-to-point test between your Switch and another IEEE 802.3-compliant device on your network. These tests can tell you whether the Switch is communicating properly with another device.

Note: To respond to a Ping test or a Link test, the device you are trying to reach must be IEEE 802.3-compliant.

This is a test of the path between the Switch and another device on the same or another IP network that can respond to IP packets (ICMP Echo Requests).

10.7.2 CLI: Ping Test

Ping Test. You can issue single or multiple ping tests with varying repetitions or counts and timeout periods. The defaults and ranges are:

_ Count: 1 (1 - 999)
_ Timeout: 5 seconds (1 - 256 seconds)
Syntax: ping <*ip-address*> [count <1 - 999>] [timeout <1 - 256>]

Example: Magnum 6K25> **ping 192.168.1.10**
Your response will be 192.168.1.10 is alive, time=15ms

Example 2: Magnum 6K25> **ping 192.168.1.10 count=3**
Your response will be 192.168.1.10 is alive, time=15ms
192.168.1.10 is alive, time=15ms
192.168.1.10 is alive, time=15ms

You can do any combination of the above IP address, count, and timeout commands.

To halt a ping test before it concludes, press [Ctrl] [C].

10.8 CLI Administrative and Troubleshooting Commands

These commands provide information or perform actions that you may find helpful in troubleshooting operating problems with the Switch.

Note For more on the CLI, refer to chapter 2, "Using the Command Line Reference (CLI).

Type Syntax: **show version** shows the software version currently running on the Switch.
Similarly *Type Syntax*: **show history** Displays the current command history.
Type Syntax: **show setup** Displays the Switch Setup screen.
Type Syntax: **!!** Repeatedly executes the previous command.

APPENDIX A

Daylight Savings Time on Magnum Switches

Magnum6K Switches provide a way to automatically adjust the system clock for Daylight Savings Time (DST) changes. The
user defines the month and date to begin and end the change from standard time. In addition to the value "none" (no time changes), there are fifteen pre-defined settings, a few examples are:

- Alaska
- Canada and Continental US
- Middle Europe and Portugal
- Southern Hemisphere
- Western Europe

The pre-defined settings follow these rules:

Alaska:

• Begin DST at 2am the first Sunday on or after April 24th.
• End DST at 2am the first Sunday on or after October 25th.

Canada and Continental US:

• Begin DST at 2am the first Sunday on or after April 1st.
• End DST at 2am the first Sunday on or after October 25th.

Middle Europe and Portugal:

• Begin DST at 2am the first Sunday on or after March 25th.
• End DST at 2am the first Sunday on or after September 24th.

Southern Hemisphere:

• Begin DST at 2am the first Sunday on or after October 25th.
• End DST at 2am the first Sunday on or after March 1st.

Western Europe:

• Begin DST at 2am the first Sunday on or after March 23rd.
• End DST at 2am the first Sunday on or after October 23rd.

A sixth option named "User defined" allows the user to customize the DST configuration by entering the beginning month and date plus the ending month and date for the time change.

Before configuring a "User defined" Daylight Time Rule, it is important to understand how the Switch treats the entries. The Switch knows which dates are Sundays, and uses an algorithm to determine on which date to change the system clock, given the configured "Beginning day" and "Ending day":

?? If the configured day is a Sunday, the time changes at 2am on that day.
?? If the configured day is not a Sunday, the time changes at 2am on the first Sunday after the configured day.

This is true for both the "Beginning day" and the "Ending day".

Here is the list of valid country codes to set daylight settings.

- Egypt
- Namibia
- USSR
- Iraq
- Lebanon
- Syria
- Australia
- London
- Belgium
- Italy
- Greece
- Cuba
- USA
- Falklands
- Chile

APPENDIX B

How to Upgrade

Magnum 6K25 Managed Network Software (MNS) can be obtained from GarrettCom FTP site (ftp.garrettcom.com)
Username: ftpuser, Password: ftpuser and uploaded to the Magnum 6K25 Switch unit. The upgrade feature of the Magnum 6K25 is provided for facilitating periodic MNS Software upgrades.

MNS Software Download from FTP site

Downloading Magnum 6K25 software (MNS) from GarrettCom's FTP site (ftp.garrettcom.com

a. Use browser (Microsoft Internet Explorer or Netscape Navigator) or any FTP tools to
download the MNS Software.
b. If you use browser interface, use the following URL to access the files:
ftp://ftp.garrettcom.com
c. If you are using an FTP client program, connect to **ftp.garrettcom.com**
d. User: ftpuser ; password: ftpuser
e. Download the MNS Software on your Desktop PC (Chosen to be used as a console terminal)

Assumptions:

?? The responsible person configuring this switch is well versed with Hyper Terminal (Windows 98, 2000, XP) or Minicom (Linux).

Note: For Linux/Unix Minicom Configuration instructions, please refer to page g below.

?? The 6K25 Switch must be connected via the console RS-232 port (located on the right rear of the unit as shown in Fig 1.0) to a serial port of a Desktop PC operating as a console terminal.

Note:(*The DB-9 (Null Modem) connecting cable is required for the connection. It is not supplied along with the Magnum6K25 unit*). It can be purchased from any Electronic Store.

Connecting the Console Terminal to Magnum6K

Use the DB-9 cable to connect the Magnum6K25 Switch Console (RS-232) port to the Desktop PC (Console Terminal).

Caution: While connecting the DB9 cable to the Magnum6K25 unit, the unit must be switched off.

On Desktop PC (Windows Console)

Follow these steps to connect the Desktop PC or terminal to the Magnum6K25 Switch:

Step 1: Using the DB9 cable, connect to the Magnum 6K25 console port, as shown in the Fig. 1.0 below

Rear View of Magnum 6K25

Fig 1.0

Step 2: Attach the other end of the DB-9 female adapter to the Desktop PC (COM1, COM2 or COM3 Port).

Step 3: Run Hyper Terminal on the Desktop PC.

Step 4: Provide an appropriate name and Press **OK** then connect to the serial port using COM1, COM2 or COM3 (as provided on Desktop PC) and Press **OK.**

Step 5: Configure the following parameters as shown in the Fig 1.0:

?? 38400 baud
?? 8 data bits
?? 1 stop bit
?? No parity
?? None

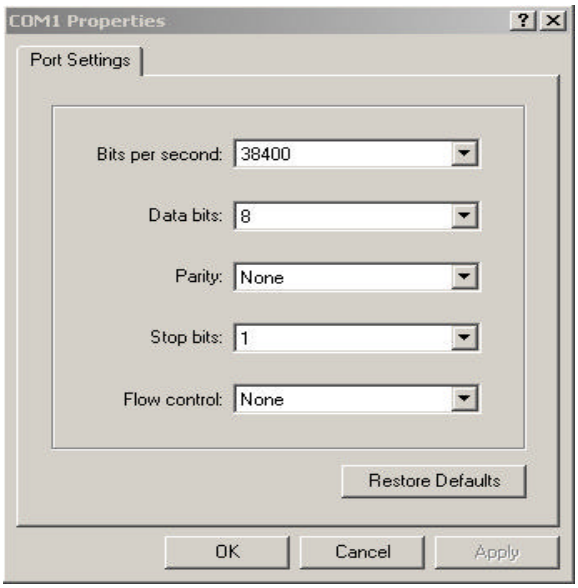


Fig 2.0

Step 6: Power on the Magnum6K25 Switch and obtain the Magnum6K25(boot)# prompt on the *Hyper Terminal* window.

Step 7: Invoke the **upgrade** command by typing "upgrade" without any arguments and press enter key as shown below.

Magnum6K25(boot)# **upgrade** *<enter>*

Step 8: From the *Hyper Terminal Menu*, Select **Transfer -> Send File** -> a small popup window opens... use **Browse** button to locate your path to the MNS Software file (Rel1.0.srec) location, and select the protocol as **Xmodem** from the drop down list, then **click Ok.**

Step 9: The download starts and proceeds to download the file. You will get the message " Upgrade is Successful. Please reboot Magnum6K25 now to start the application" at the end. If there is any error in the file transfer, you will get the error message " Upgrade failed " and the program will abort back to the (boot) prompt.
NOTE: Please do not interrupt the Magnum6K25 unit or the Desktop PC during the download process. If for any reason the download is not complete, please follow steps 6 through 9 again to complete the upgrade process.

On Linux Console

Step 1: Run Minicom.

Step 2: To set the baud rate of the COM Port. Press <ctrl> A …Z…P…G and <Enter>

Step 3: Power on the Magnum6K Switch. You will see the Boot Prompt Magnum6K25 (boot)#

Step 4: Invoke the **upgrade** command by typing "upgrade" without any arguments and press enter key as shown below.

Magnum6K25(boot)# **upgrade** *<enter>*

Step 5: Press <ctrl>A…S, Select *xmodem* from the Popup window and press <enter>. Select [Go To] Tab and <Enter>

Step 6: You will get the window asking for the Directory. Give the full path of the directory where you have copied the Image file to upload and press <enter>.

Step 7: Select the file with the help of the spacebar and Press <Enter>. The download starts and proceeds to download the file.… At the end of the transfer close the progress indicator window.

Step 8: The download starts and proceeds to download the file. You will get the message " Upgrade is Successful. Please reboot Magnum6K25 now to start the application" at the end. If there is any error in the file transfer, you will get the error message " Upgrade failed " and the program will abort back to the (boot) prompt.

To Check the Successful Upgrade:

Once you restart the switch, you will get the **login** prompt on the Hyper Terminal (as shown below).

```
Copyright (c) 2001 GarrettCom, Inc. All rights reserved.

RESTRICTED RIGHTS
-----------------
Use, duplication or disclosure is subject to U.S. Government restrictions
as set forth in Sub-division (b)(3)(ii) of the rights in Technical Data and
Computer Software clause at 52.227-7013.

   GarrettCom, Inc.
   213, Hammond Avenue,
   Fremont,
   CA 94539,
   United States (USA)
   www.garrettcom.com
Magnum6K25 build Jan 14 2002,12:12:53

login:
```